

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

SUBJECT PREMISES,
SUBJECT VEHICLE 1 and SUBJECT VEHICLE 2

Case No. MJ21-140

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Subject Premises and Subject Vehicles 1 & 2 and as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18 U.S.C. § 2252(a)(2)
Title 18 U.S.C. § 2252(a)(4)(B)

Offense Description

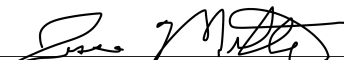
Receipt/Distribution of Child Pornography
Possession of Child Pornography

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

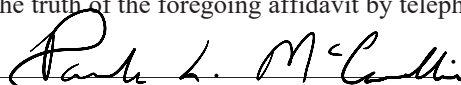
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Special Agent Jesse Miller, HSI
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/08/2021


Judge's signature

City and state: Bellingham, Washington

Paula L. McCandlis, United States Magistrate Judge
Printed name and title

ATTACHMENT A**Description of Property to be Searched**

The physical address of the SUBJECT PREMISES is 3407 Woburn Street, Apartment 112, Bellingham, Washington 98226, and is more fully described as an apartment within a multi-unit dwelling. The door of Apartment 112 is black and bears the number "112"

The search is to include all rooms and persons within the SUBJECT PREMISES and all garage/parking spaces, or storage areas assigned to Apartment 112, as well as any digital device(s) found therein.





Description of the SUBJECT VEHICLES

SUBJECT VEHICLE 1 is a 2016 Grand Caravan , bearing Washington License Plate #BHR0403.

SUBJECT VEHICLE 2 is a 2014 Volkswagen Jetta, bearing Washington License Plate #AR14245.

The search of SUBJECT VEHICLES 1 and 2 is to include the entirety of the vehicles, any close containers, and any digital devices found therein.

ATTACHMENT B**ITEMS TO BE SEIZED**

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) committed in or after November 2020 as follows:

- a. Items, records, or information³ relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- c. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- d. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- e. Items, records, or information related to communications with or about minors;
- f. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- g. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence,

³ As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

1 purchase or lease agreements, diaries, statements, identification documents,
2 address books, telephone directories, and keys;

3 h. Items, records, or information concerning the ownership or use of computer
4 equipment found in the SUBJECT PREMISES, including, but not limited
5 to, sales receipts, bills for internet access, handwritten notes, and computer
6 manuals;

7 i. Any digital devices or other electronic storage media⁴ and/or their
8 components including:

9 i. any digital device or other electronic storage media capable of being
10 used to commit, further, or store evidence, fruits, or instrumentalities
11 of the offenses listed above;

12 ii. any magnetic, electronic or optical storage device capable of storing
13 data, including thumb drives, SD cards, or external hard drives;

14 iii. any physical keys, encryption devices, dongles and similar physical
15 items that are necessary to gain access to the computer equipment,
16 storage devices or data; and

17 iv. any passwords, password files, test keys, encryption codes or other
18 information necessary to access the computer equipment, storage
19 devices or data.

20 j. For any digital device or other electronic storage media whose seizure is
21 otherwise authorized by this warrant, and any digital device or other
22 electronic storage media that contains or in which is stored records or
23 information that is otherwise called for by this warrant:

24 i. evidence of who used, owned, or controlled the digital device or
25 other electronic storage media at the time the things described in this
26 warrant were created, edited, or deleted, such as logs, registry
27 entries, configuration files, saved usernames and passwords,
28

26 ⁴ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical,
27 or other high speed data processing devices performing logical, arithmetic, or storage functions,
28 including desktop computers, notebook computers, mobile phones, tablets, server computers, and
network hardware. The term “electronic storage media” includes any physical object upon
which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash
memory, CD-ROMs, and other magnetic or optical media.

documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- ii. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- iii. evidence of the lack of such malicious software;
- iv. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
- v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
- vi. evidence of the times the digital device or other electronic storage media was used;
- vii. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
- viii. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;
- ix. records of or information about the Internet Protocol used by the digital device or other electronic storage media;
- x. records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.
- xi. contextual information necessary to understand the evidence described in this attachment.

1 This warrant authorizes a review of electronic storage media and electronically stored
2 information seized or copied pursuant to this warrant in order to locate evidence, fruits,
3 and instrumentalities described in this warrant. The review of this electronic data may be
4 conducted by any government personnel assisting in the investigation, who may include,
5 in addition to law enforcement officers and agents, attorneys for the government, attorney
6 support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete
7 copy of the seized or copied electronic data to the custody and control of attorneys for the
8 government and their support staff for their independent review.

9 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
10 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
11 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
12 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
13 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
14 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
15 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
16 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
17 CRIMES.
18
19
20
21
22
23
24
25
26
27
28

I, Jesse Miller, being duly sworn on oath, depose and state:

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent since 2001. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2018, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI (formally known as the U.S. Customs Service) Special Agent Training Program and have received further specialized training in investigating child pornography and child exploitation crimes. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have participated in the execution of many search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. I am a member of the Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of

1 crimes involving the sexual exploitation of children. In April of 2018, I completed a
 2 ICAC sponsored training in the BitTorrent (P2P) file sharing program.

3 PURPOSE OF AFFIDAVIT

4 2. I make this affidavit in support of an application under Rule 41 of the
 5 Federal Rules of Criminal Procedure for a search warrant for the following location, as
 6 further described in Attachment A:

7 a. 3407 Woburn Street, Apartment 112, Bellingham, Washington 98226 (the
 8 SUBJECT PREMISES)

9 b. 2016 Grand Caravan, with Washington License Plate #BHR0403,
 10 (SUBJECT VEHICLE 1)

11 c. 2014 Volkswagen Jetta, with Washington License Plate #AR14245,
 12 (SUBJECT VEHICLE 2)

13 3. As set forth below, there is probable cause to believe that the SUBJECT
 14 PREMISES and SUBJECT VEHICLES will contain or possess evidence, fruits, and
 15 instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child
 16 Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography)
 17 (hereinafter the "TARGET OFFENSES"). I seek authorization to search and seize the
 18 items specified in Attachment B, which is incorporated herein by reference.

19 4. The information in this affidavit is based upon the investigation I have
 20 conducted in this case, my conversations with other law enforcement officers who have
 21 engaged in various aspects of this investigation, and my review of reports written by
 22 other law enforcement officers involved in this investigation. Because this affidavit is
 23 being submitted for the limited purpose of securing search warrants, I have not included
 24 each and every fact known to me concerning this investigation. I have set forth only
 25 those facts that I believe are sufficient to establish probable cause to support the issuance
 26 of the requested warrants. When the statements of others are set forth in this affidavit,
 27 they are set forth in substance and in part.

1 5. This Affidavit is being presented electronically pursuant to Local Criminal
2 Rule CrR 41(d)(3).

3 **PEER-TO-PEER (P2P) FILE SHARING**

4 6. Peer to peer (P2P) file sharing is a method of communication available to
5 internet users through the use of special software programs. P2P file sharing programs
6 allow groups of computers using the same file sharing network and protocols to transfer
7 digital files from one computer system to another while connected to a network, usually
8 on the internet. There are multiple types of P2P file sharing networks on the internet. To
9 connect to a particular P2P file sharing network, a user first obtains a P2P client software
10 program for a particular P2P file sharing network, which can be downloaded from the
11 internet. A particular P2P file sharing network may have many different P2P client
12 software programs that allow access to that particular P2P file sharing network.
13 Additionally, a particular P2P client software program may be able to access multiple
14 P2P file sharing networks. These P2P client software share common protocols for
15 network access and file sharing. The user interface, features, and configurations may
16 vary between clients and versions of the same client.

17 7. In general, P2P client software allows the user to set up file(s) on a
18 computer to be shared on a P2P file sharing network with other users running compatible
19 P2P client software. A user can also obtain files by opening the P2P client software on
20 the user's computer and conducting a search for files that are of interest and currently
21 being shared on a P2P file sharing network.

22 8. Some P2P file sharing networks are designed to allow users to download
23 files and frequently provide enhanced capabilities to reward the sharing of files by
24 providing reduced wait periods, higher user ratings, or other benefits. In some instances,
25 users are not allowed download files if they are not sharing files. Typically, settings
26 within these programs control sharing thresholds.

27 9. Typically, during a default installation of a P2P client software program,
28 settings are established which configure the host computer to share files. Depending

1 upon the P2P client software used, a user may have the ability to reconfigure some of
2 those settings during installation or after the installation has been completed.

3 10. Typically, a setting establishes the location of one or more directories or
4 folders whose contents (digital files) are made available for distribution to other P2P
5 clients. In some clients, individual files can also be shared.

6 11. Typically, a setting controls whether or not files are made available for
7 distribution to other P2P clients.

8 12. Typically, a setting controls whether or not users will be able to share
9 portions of a file while they are in the process of downloading the entire file. This feature
10 increases the efficiency of the network by putting more copies of the file segments on the
11 network for distribution.

12 13. Typically, files being shared by P2P clients are processed by the client
13 software. As part of this processing, a hashed algorithm value is computed for each file
14 and/or piece of a file being shared (dependent on the P2P file sharing network), which
15 uniquely identifies it on the network. A file (or piece of a file) processed by this hash
16 algorithm operation results in the creation of an associated hash value often referred to as
17 a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent
18 that two or more files with the same hash value are identical copies of the same file
19 regardless of their file names. By using a hash algorithm to uniquely identify files on a
20 P2P network, it improves the network efficiency. Because of this, typically, users may
21 receive a selected file from numerous sources by accepting segments of the same file
22 from multiple clients and then reassembling the complete file on the local computer.
23 This is referred to as multiple source downloads. This client program succeeds in
24 reassembling the file from different sources only if all the segments came from exact
25 copies of the same file. P2P file sharing networks use hash values to ensure exact copies
26 of the same files are used during this process.

1 14. P2P file sharing networks, including the BitTorrent network, are frequently
2 used to trade digital files of child pornography. These files include both images and
3 movie files.

4 15. The BitTorrent network is a very popular and publicly available P2P
5 sharing network. Most computers that are part of this network are referred to as “peers.”
6 The terms “peers” and “clients” can be used interchangeably when referring to the
7 BitTorrent network. A peer can simultaneously provide files to some peers while
8 downloading files from other peers.

9 16. The BitTorrent network can be accessed by computers running many
10 different client programs, some of which include the BitTorrent client program, uTorrent
11 client program, and Vuze client program. These client programs are publicly available
12 and free P2P client software programs that can be downloaded from the internet. There
13 are also BitTorrent client programs that are not free. These BitTorrent client programs
14 share common protocols for network access and file sharing. The user interfaces,
15 features, and configuration may vary between clients and versions of the same client.

16 17. During the installation of typical BitTorrent network client programs,
17 various settings are established which configure the host computer to share files.
18 Depending upon the BitTorrent client used, a user may have the ability to reconfigure
19 some of those settings during installation or after installation has been completed.
20 Typically, a setting establishes the location of one or more directories of folders whose
21 contents (files) are made available to other BitTorrent network users to download.

22 18. In order to share a file or set of files on a BitTorrent network, a “Torrent”
23 file needs to be created by the user that initially wants to share the file or set of files. A
24 “Torrent” is typically a small file that describes the file(s) that are being shared, which
25 may include information on how to locate the file(s) on the BitTorrent network. A
26 typical BitTorrent client will have the ability to create a “Torrent” file. It is important to
27 note that the “Torrent” file does not contain the actual file(s) being shared, but
28 information about the file(s) described in the “Torrent,” such as the name(s) of the file(s)

1 being referenced in the “Torrent” and the “info hash” of the “Torrent.” The “info hash”
2 is a SHA-1 hash value of the set of data describing the file(s) referenced in the “Torrent,”
3 which include the SHA-1 hash value of each piece, the file size, and the file name(s).
4 The “info hash” of each “Torrent” uniquely identifies the “Torrent” file on the BitTorrent
5 network. The “Torrent” file may also contain information on how to locate file(s)
6 referenced in the “Torrent” by identifying “Trackers.” “Trackers” are computers on the
7 BitTorrent network that collate information about peers/clients that have recently
8 reported they are sharing the file(s) referenced in the “Torrent” file. A “Tracker” is only
9 a pointer to peers/clients on the network who may be sharing part or all of the file(s)
10 referenced in the “Torrent.” It is important to note that the “Trackers” do not actually
11 have the file(s) and are used to facilitate the finding of other peers/clients that have the
12 entire file(s) or at least a portion of the file(s) available for sharing. It should also be
13 noted that the use of “Tracker(s)” on the BitTorrent network are not always necessary to
14 locate peers/clients that have file(s) being shared from a particular “Torrent” file. There
15 are many publicly available servers on the Internet that provide BitTorrent tracker
16 services.

17 19. Once a “Torrent” is created, in order to share the file(s) referenced in the
18 “Torrent” file, a user typically makes the “Torrent” available for other users, such as via
19 websites on the Internet.

20 20. In order to locate “Torrent” files of interest, a typical user will use keyword
21 searches within the BitTorrent network client itself or on websites hosting “Torrents.”
22 Once a “Torrent” file is located that meets the keyword search criteria, the user will
23 download the “Torrent” file to their computer. Alternatively, a user can also search for
24 and locate “magnet links,” which is a link that enables the BitTorrent network client
25 program itself to download the “Torrent” to the computer. In either case, a “Torrent” file
26 is downloaded to the user’s computer. The BitTorrent network client will then process
27 that “Torrent” file in order to find “Trackers” or utilize other means that will help
28 facilitate finding other peers/clients on the network that have all or part of the file(s)

1 referenced in the “Torrent” file. It is again important to note that the actual file(s)
2 referenced in the “Torrent” are actually obtained directly from other peers/clients on the
3 BitTorrent network and not the “Trackers” themselves. Typically, the “Trackers” on the
4 network return information about remote peers/clients that have recently reported they
5 have the same file(s) available for sharing (based on SHA-1 “info hash” value
6 comparison), or parts of the same file(s), referenced in the “Torrent,” to include the
7 remote peers/clients Internet Protocol (IP) addresses.

8 21. For example, a person interested in obtaining child pornographic images on
9 the BitTorrent network would open the BitTorrent client application on his/her computer
10 and conduct a keyword search for files using a term such as “preteen sex.” (It should be
11 noted that this search term may not have been used in this investigation.) The results of
12 the torrent search are typically returned to the user’s computer by displaying them on the
13 torrent hosting website. The hosting website will typically display information about the
14 torrent, which can include the name of the torrent file, the name of the file(s) referenced
15 in the torrent file, the file(s) size, and the “info hash” SHA-1 value of the torrent file.
16 The user then selects a torrent of interest to download to their computer. Typically, the
17 BitTorrent client program will then process the torrent file. The user selects from the
18 results displayed the file(s) they want to download that were referenced in the torrent file.
19 Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash
20 Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have
21 recently reported they have the file(s) or parts of the file(s) referenced in the torrent file
22 available for sharing. The file(s) is then downloaded directly from the computer(s)
23 sharing the file. Typically, once the BitTorrent network client has downloaded part of the
24 file(s), it may immediately begin sharing the file with other users on the network. The
25 BitTorrent network client program succeeds in reassembling the file(s) from different
26 sources only if it receives “pieces” with the exact SHA-1 piece hash described in the
27 torrent file. During the download process, a typical BitTorrent client program displays
28 the Internet Protocol address of the peers/clients that appear to be sharing part or all of

1 the file(s) referenced in the torrent file or other methods utilized by the BitTorrent
2 network protocols. The downloaded file is then stored in the area previously designated
3 by the user and/or the client program. The downloaded file(s), including the torrent file,
4 will remain until moved or deleted.

5 22. Law Enforcement has created BitTorrent network client programs that
6 obtain information from trackers about peers/clients recently reporting that they are
7 involved in sharing digital files of known actual child pornography (based on the “info
8 hash” SHA-1 hash value), which then allows the downloading of a file from a single IP
9 address (as opposed to obtaining the file from multiple peers/clients on the network.)
10 This procedure allows for the detection and investigation of those computers involved in
11 sharing digital files of known actual child pornography on the BitTorrent network.

12 23. During the query and/or downloading process from a remote BitTorrent
13 network client, certain information may be exchanged between the investigator’s client
14 and the remote client they are querying and/or downloading a file from. Such as 1) the
15 remote client’s IP address; 2) a confirmation from the remote client that they have pieces
16 of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being
17 reported as shared from the remote client program; and 3) the remote client program and
18 version. This information may remain on the remote client’s computer system for long
19 periods of time. The investigator has the ability to log this information. A search can
20 later be conducted on a seized computer system(s) for this information, which may
21 provide further evidence that the investigator’s client communicated with the remote
22 client.

23 **STATEMENT OF PROBABLE CAUSE**

24 24. Between November 2020 and February 2021, I used a law enforcement
25 version of BitTorrent to identify P2P users possessing and distributing image and video
26 files depicting child pornography. I used the law enforcement version of BitTorrent to
27 download files depicting child pornography from a P2P user at IP address 76.121.47.160
28 (the SUBJECT IP ADDRESS). The undercover downloads are detailed below.

25. On November 30, 2020, between approximately 1:16 a.m. PST and 2:21 a.m. PST, I used the law enforcement version of BitTorrent to establish a single source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of suspected child pornography. Among the files downloaded from the SUBJECT IP ADDRESS was the following video file that I reviewed and describe below:

File: This video is 14 minute and 06 second long. The video depicts a nude, prepubescent female performing oral sex on an artificial phallus, with camera views of her breasts and vagina. Given her small stature, lack of pubic development/pubic and body hair, minimal to no breast development, and youthful appearances, I estimate the young girl is between ten and twelve years old.

26. On February 13, 2021, between approximately 8:21 a.m. PST and February 14, 2021 12:54 a.m. PST, I used the law enforcement version of BitTorrent to establish a single source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of suspected child pornography. Among the files downloaded from the SUBJECT IP ADDRESS were the following videos, which I reviewed and describe below:

File 1: This video is 16 minutes and 41 seconds long and depicts a nude prepubescent female. During the video, the adult male subjects the child victim to oral and vaginal sexual intercourse and ejaculates in the child victim's mouth at the conclusion of the video. Given her small stature, lack of pubic development/pubic and body hair, minimal to no breast development, and youthful appearance, I estimate the young girl is between nine and eleven years old.

File 2: This video is 9 minutes and 55 seconds long and depicts a nude, prepubescent female in the backseat of a vehicle with a nude adult male. The child is digitally penetrated in her vagina and anus. Later in the video the adult male's erect penis is inserted in the child's anus. Several times in the video, the child victim's face is visible and she appears to be in distress. Given her small stature, lack of pubic development, minimal to no breast development, and youthful appearance, I estimate the young girl is between eight and ten years old.

27. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to Comcast Communications. Comcast was served a U.S.

1 Department of Homeland Security summons seeking subscriber information of the
2 SUBJECT IP ADDRESS from November 2020 to February 2021. Comcast
3 Communications reported during the dates and times of the downloads described above,
4 the SUBJECT IP ADDRESS was assigned to Irina Yakimyuk with a service and billing
5 address at the SUBJECT PREMISES, an apartment within a multi-unit building.

6 28. On March 2, 2021, law enforcement conducted surveillance on the
7 SUBJECT PREMISES and saw a vehicle registered to Irina Yakimyuk parked in front of
8 the apartment building numbered "3407" and near apartment 112, the SUBJECT
9 PREMISES.

10 29. Washington State Department of License records show that Irina Yakimyuk
11 and James Phelps list the SUBJECT PREMISES as their current residential address.
12 From my investigation, I believe they are the only adult residents of the SUBJECT
13 PREMISES. But I believe a minor female under the age of twelve also resides at the
14 SUBJECT PREMISES.

15 30. Washington DOL records also show that SUBJECT VEHICLE 1 is
16 currently registered to Irina Yakimyuk and James Phelps and SUBJECT VEHICLE 2 is
17 currently registered to James Phelps . Both are registered at the SUBJECT PREMISES.

18 31. Based on my knowledge, training, and experience, and the experience of
19 other law enforcement officers, I know that it is common for multiple individuals and
20 computers within a residence to share Internet access. I believe that someone used at
21 least one computer from the SUBJECT PREMISES to distribute child pornography via
22 an Internet based P2P file sharing program, and that evidence of that crime will be found
23 in the SUBJECT PREMISES or in the SUBJECT VEHICLES.

24 **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

25 32. I have had both training and experience in the investigation of computer-
26 related crimes. Based on my training, experience, and knowledge, I know the following:
27
28

1 a. Computers and digital technology are the primary way in which
2 individuals interested in child pornography interact with each other. Computers basically
3 serve four functions in connection with child pornography: production, communication,
4 distribution, and storage.

5 b. Digital cameras and smartphones with cameras save photographs or
6 videos as a digital file that can be directly transferred to a computer by connecting the
7 camera or smartphone to the computer, using a cable or via wireless connections such as
8 “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may
9 be stored on a removable memory card in the camera or smartphone. These memory
10 cards are often large enough to store thousands of high-resolution photographs or videos.

11 c. A device known as a modem allows any computer to connect to
12 another computer through the use of telephone, cable, or wireless connection. Mobile
13 devices such as smartphones and tablet computers may also connect to other computers
14 via wireless connections. Electronic contact can be made to literally millions of
15 computers around the world. Child pornography can therefore be easily, inexpensively
16 and anonymously (through electronic communications) produced, distributed, and
17 received by anyone with access to a computer or smartphone.

18 d. The computer’s ability to store images in digital form makes the
19 computer itself an ideal repository for child pornography. Electronic storage media of
20 various types - to include computer hard drives, external hard drives, CDs, DVDs, and
21 “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a
22 port on the computer - can store thousands of images or videos at very high resolution. It
23 is extremely easy for an individual to take a photo or a video with a digital camera or
24 camera-bearing smartphone, upload that photo or video to a computer, and then copy it
25 (or any other files on the computer) to any one of those media storage devices. Some
26 media storage devices can easily be concealed and carried on an individual’s person.
27 Smartphones and/or mobile phones are also often carried on an individual’s person.

28 e. The Internet affords individuals several different venues for
obtaining, viewing, and trading child pornography in a relatively secure and anonymous
fashion.

 f. Individuals also use online resources to retrieve and store child
pornography. Some online services allow a user to set up an account with a remote
computing service that may provide email services and/or electronic storage of computer
files in any variety of formats. A user can set up an online storage account (sometimes
referred to as “cloud” storage) from any computer or smartphone with access to the
Internet. Even in cases where online storage is used, however, evidence of child
pornography can be found on the user’s computer, smartphone, or external media in most
cases.

1 g. A growing phenomenon related to smartphones and other mobile
2 computing devices is the use of mobile applications, also referred to as “apps.” Apps
3 consist of software downloaded onto mobile devices that enable users to perform a
4 variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or
5 playing a game – on a mobile device. Individuals commonly use such apps to receive,
6 store, distribute, and advertise child pornography, to interact directly with other like-
minded offenders or with potential minor victims, and to access cloud-storage services
where child pornography may be stored.

7 h. As is the case with most digital technology, communications by way
8 of computer can be saved or stored on the computer used for these purposes. Storing this
9 information can be intentional (i.e., by saving an email as a file on the computer or saving
10 the location of one’s favorite websites in, for example, “bookmarked” files) or
11 unintentional. Digital information, such as the traces of the path of an electronic
12 communication, may also be automatically stored in many places (e.g., temporary files or
13 ISP client software, among others). In addition to electronic communications, a
computer user’s Internet activities generally leave traces or “footprints” in the web cache
and history files of the browser used. Such information is often maintained indefinitely
until overwritten by other data.

14 33. Based upon my knowledge, experience, and training in child pornography
15 investigations, and the training and experience of other law enforcement officers with
16 whom I have had discussions, I know that there are certain characteristics common to
17 individuals who have a sexualized interest in children and depictions of children:
18
19
20
21
22
23
24
25
26
27
28

1 a. They may receive sexual gratification, stimulation, and satisfaction
2 from contact with children; or from fantasies they may have viewing children engaged in
3 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
4 visual media; or from literature describing such activity.

5 b. They may collect sexually explicit or suggestive materials in a
6 variety of media, including photographs, magazines, motion pictures, videotapes, books,
7 slides, and/or drawings or other visual media. Such individuals often times use these
8 materials for their own sexual arousal and gratification. Further, they may use these
9 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
10 selected child partner, or to demonstrate the desired sexual acts. These individuals may
11 keep records, to include names, contact information, and/or dates of these interactions, of
12 the children they have attempted to seduce, arouse, or with whom they have engaged in
13 the desired sexual acts.

14 c. They often maintain any “hard copies” of child pornographic
15 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
16 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
17 their home or some other secure location. These individuals typically retain these “hard
18 copies” of child pornographic material for many years, as they are highly valued.

19 d. Likewise, they often maintain their child pornography collections
20 that are in a digital or electronic format in a safe, secure and private environment, such as
21 a computer and surrounding area. These collections are often maintained for several
22 years and are kept close by, often at the individual’s residence or some otherwise easily
23 accessible location, to enable the owner to view the collection, which is valued highly.

24 e. They also may correspond with and/or meet others to share
25 information and materials; rarely destroy correspondence from other child pornography
26 distributors/collectors; conceal such correspondence as they do their sexually explicit
27 material; and often maintain lists of names, addresses, and telephone numbers of
28 individuals with whom they have been in contact and who share the same interests in
child pornography.

1 f. They generally prefer not to be without their child pornography for
2 any prolonged time period. This behavior has been documented by law enforcement
3 officers involved in the investigation of child pornography throughout the world.
4 Importantly, e-mail and cloud storage can be a convenient means by which individuals
5 can access a collection of child pornography from any computer, at any location with
6 Internet access. Such individuals therefore do not need to physically carry their
7 collections with them but rather can access them electronically. Furthermore, these
8 collections can be stored on email “cloud” servers, which allow users to store a large
9 amount of material at no cost, and possibly reducing the amount of any evidence of any
10 of that material on the users’ computer(s).

11 34. Even if such individuals use a portable device (such as a mobile phone) to
12 access the Internet and child pornography, it is more likely than not that evidence of this
13 access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment
14 A, including on digital devices other than the portable device (for reasons including the
15 frequency of “backing up” or “synching” mobile phones to computers or other digital
16 devices).

17 35. In addition to offenders who collect and store child pornography, law
18 enforcement has encountered offenders who obtain child pornography from the internet,
19 view the contents and subsequently delete the contraband, often after engaging in self-
20 gratification. In light of technological advancements, increasing Internet speeds and
21 worldwide availability of child sexual exploitative material, this phenomenon offers the
22 offender a sense of decreasing risk of being identified and/or apprehended with quantities
23 of contraband. This type of consumer is commonly referred to as a ‘seek and delete’
24 offender, knowing that the same or different contraband satisfying their interests remain
25 easily discoverable and accessible online for future viewing and self-gratification. I
26 know that, regardless of whether a person discards or collects child pornography he/she
27 accesses for purposes of viewing and sexual gratification, evidence of such activity is
28 likely to be found on computers and related digital devices, including storage media, used
by the person. This evidence may include the files themselves, logs of account access
events, contact lists of others engaged in trafficking of child pornography, backup files,
and other electronic artifacts that may be forensically recoverable.

36. Given the above-stated facts, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the person who used a computer at the SUBJECT PREMISES to share the files described above likely has a sexualized interest in children and depictions of children, and that evidence of child pornography is likely to be found at the SUBJECT PREMISES or in the SUBJECT VEHICLES.

FRUITS, EVIDENCE, AND INSTRUMENTALITIES INSIDE THE SUBJECT PREMISES/SUBJECT VEHICLES AND ANY CLOSED CONTAINERS AND ELECTRONIC DEVICES FOUND THEREIN

37. As described above and in Attachment B, this application seeks permission to search for and seize items listed in Attachment B that might be found in the SUBJECT PREMISES or in the SUBJECT VEHICLES, in whatever form they are found. One form in which evidence, fruits, or instrumentalities might be found is data stored on a computer's hard drive or other digital device¹ or electronic storage media.² Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

38. Through my training and experience, and the information learned during the course of this investigation, I know that individuals who engage in child pornography offenses often keep physical evidence, fruits, and instrumentalities of their crimes inside their residences, including but not limited to, digital devices

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 39. *Probable cause.* Based upon my review of the evidence gathered in this
2 investigation, my review of data and records, information received from other agents and
3 computer forensic examiners, and my training and experience, I submit that if a digital
4 device or other electronic storage medium is found in the SUBJECT PREMISES or
5 SUBJECT VEHICLES, there is probable cause to believe that evidence, fruits, and
6 instrumentalities of the TARGET OFFENSES will be stored on those digital devices or
7 other electronic storage media. As noted above, my investigation has shown that the user
8 of a computer at the SUBJECT PREMISES has shared suspected child pornography.
9 There is, therefore, probable cause to believe that evidence, fruits, and instrumentalities,
10 of the crimes under investigation exist and will be found on digital devices or other
11 electronic storage media at the SUBJECT PREMISES or in the SUBJECT VEHICLES
12 for at least the following reasons:

1 a. Based my knowledge, training, and experience, I know that
 2 computer files or remnants of such files may be recovered months or even years after
 3 they have been downloaded onto a storage medium, deleted, or viewed via the Internet.
 4 Electronic files downloaded to a storage medium can be stored for years at little or no
 5 cost. Even when files have been deleted, this information can sometimes be recovered
 6 months or years later with forensics tools. This is because when a person “deletes” a file
 on a computer, the data contained in the files does not actually disappear; rather, that data
 remains on the storage medium until it is overwritten by new data.

7 b. Therefore, deleted files, or remnants of deleted files, may reside in
 8 free space or slack space—that is, in space on the storage medium that is not currently
 9 being used by an active file—for long periods of time before they are overwritten. In
 10 addition, a computer’s operating system may also keep a record of deleted data in “swap”
 or “recovery” files.

11 c. Wholly apart from user-generated files, computer storage media—in
 12 particular, computers’ internal hard drives—contain electronic evidence of how a
 13 computer has been used, what is has been used for, and who has used it. To give a few
 14 examples, this forensic evidence can take the form of operating system configurations,
 15 artifacts from operating system or application operation, file system data structures, and
 16 virtual memory “swap” paging files. Computer users typically do not erase or delete this
 evidence, because special software is typically required for that task. However, it is
 technically possible to delete this information.

17 d. Similarly, files that have been viewed via the Internet are sometimes
 18 automatically downloaded into a temporary Internet directory or “cache.”

19 e. Digital storage devices may also be large in capacity, but small in
 20 physical size. Because those who are in possession of such devices also tend to keep
 21 them on their persons, especially when they may contain evidence of a crime. Digital
 storage devices may be smaller than a postal stamp in size, and thus they may easily be
 hidden in a person’s pocket.

22 40. As further described in Attachment B, this application seeks permission to
 23 locate not only computer files that might serve as direct evidence of the crimes described
 24 on the warrant, but also for forensic electronic evidence that establishes how computers
 25 were used, the purpose of their use, who used them, and when. There is probable cause
 26 to believe that this forensic electronic evidence will be on digital devices found in the
 27 SUBJECT PREMISES or SUBJECT VEHICLES because:
 28

1 a. Data on the digital storage medium or digital devices can provide
2 evidence of a file that was once on the digital storage medium or digital devices but has
3 since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has
4 been deleted from a word processing file). Virtual memory paging systems can leave
5 traces of information on the storage medium that show what tasks and processes were
6 recently active. Web browsers, e-mail programs, and chat programs store configuration
7 information on the storage medium that can reveal information such as online nicknames
8 and passwords. Operating systems can record additional information, such as the
9 attachment of peripherals, the attachment of USB flash storage devices or other external
10 storage media, and the times the computer was in use. Computer file systems can record
11 information about the dates files were created and the sequence in which they were
12 created, although this information can later be falsified.
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to further establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g. registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search of “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer activity associated with user accounts and electronic storage media that connected with the computer. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit the crime (e.g. Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper content, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

1 d. The process of identifying the exact files, blocks, registry entries,
 2 logs, or other forms of forensic evidence on a storage medium that are necessary to draw
 3 an accurate conclusion is a dynamic process. While it is possible to specify in advance
 4 the records to be sought, computer evidence is not always data that can be merely
 5 reviewed by a review team and passed along to investigators. Whether data stored on a
 6 computer is evidence may depend on other information stored on the computer and the
 7 application of knowledge about how a computer behaves. Therefore, contextual
 8 information necessary to understand other evidence also falls within the scope of the
 9 warrant.

10 e. Further, in finding evidence of how a computer was used, the
 11 purpose of its use, who used it, and when, sometimes it is necessary to establish that a
 12 particular thing is not present on a storage medium. For example, the presence or
 13 absence of counter-forensic programs or anti-virus programs (and associated data) may
 14 be relevant to establishing a user's intent.

15 f. I know that when an individual uses a computer to store, receive, or
 16 distribute child pornography, the individual's computer or digital device will generally
 17 serve both as an instrumentality for committing the crime, and also as a storage medium
 18 for evidence of the crime. The computer or digital device is an instrumentality of the
 19 crime because it is used as a means of committing the criminal offense. The computer or
 20 digital device is also likely to be a storage medium for evidence of crime. From my
 21 training and experience, I believe that a computer or digital device used to commit a
 22 crime of this type may contain: data that is evidence of how the computer was used; data
 23 that was sent or received; notes as to how the criminal conduct was achieved; records of
 24 text discussions about the crime; and other records that indicate the nature of the offense.

25 41. *Necessity of seizing or copying entire computers or storage medium.* In
 26 most cases, a thorough search of a premises for information that might be stored on
 27 digital storage media or other digital devices often requires the seizure of the digital
 28 devices and digital storage media for later off-site review consistent with the warrant. In
 lieu of removing storage media from the premises, it is sometimes possible to make an
 image copy of storage media. Generally speaking, imaging is the taking of a complete
 electronic copy of the digital media's data, including all hidden sectors and deleted files.
 Either seizure or imaging is often necessary to ensure the accuracy and completeness of
 data recorded on the storage media, and to prevent the loss of the data either from
 accidental or intentional destruction. This is true because of the following:

1 a. *The time required for an examination.* As noted above, not all
 2 evidence takes the form of documents and files that can be easily viewed on site.
 3 Analyzing evidence of how a computer has been used, what it has been used for, and who
 4 has used it requires considerable time, and taking that much time on premises could be
 5 unreasonable. As explained above, because the warrant calls for forensic electronic
 6 evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage
 7 media to obtain evidence. Storage media can store a large volume of information.
 8 Reviewing that information for things described in the warrant can take weeks or months,
 9 depending on the volume of data stored, and would be impractical and invasive to
 10 attempt on-site.

11 b. *Technical requirements.* Computers can be configured in several
 12 different ways, featuring a variety of different operating systems, application software,
 13 and configurations. Therefore, searching them sometimes requires tools or knowledge
 14 that might not be present on the search site. The vast array of computer hardware and
 15 software available makes it difficult to know before a search what tools or knowledge
 16 will be required to analyze the system and its data on-site. However, taking the storage
 17 media off-site and reviewing it in a controlled environment will allow its examination
 18 with the proper tools and knowledge.

19 c. *Variety of forms of electronic media.* Records sought under this
 20 warrant could be stored in a variety of storage media formats that may require off-site
 21 reviewing with specialized forensic tools.

22 42. Searching computer systems is a highly technical process that requires
 23 specific expertise and specialized equipment. There are so many types of computer
 24 hardware and software in use today that it is rarely possible to bring to the search site all
 25 the necessary technical manuals and specialized equipment necessary to consult with
 26 computer personnel who have expertise in the type of computer, operating system, or
 27 software application being searched.

28 43. The analysis of computer systems and storage media often relies on
 rigorous procedures designed to maintain the integrity of the evidence and to recover
 “hidden,” mislabeled, deceptively named, erased, compressed, encrypted or password-
 protected data, while reducing the likelihood of inadvertent or intentional loss or
 modification of data. A controlled environment such as a laboratory, is typically required
 to conduct such an analysis properly.

1 44. The volume of data stored on many computer systems and storage devices
2 will typically be so large that it will be highly impracticable to search for data during the
3 execution of the physical search of the premises. The hard drives commonly included in
4 desktop and laptop computers are capable of storing millions of pages of text.

5 45. A search of digital devices for evidence described in Attachment B may
6 require a range of data analysis techniques. In some cases, agents may recover evidence
7 with carefully targeted searches to locate evidence without requirement of a manual
8 search through unrelated materials that may be commingled with criminal evidence.
9 Agents may be able to execute a “keyword” search that searches through the files stored
10 in a digital device for special terms that appear only in the materials covered by the
11 warrant. Or, agents may be able to locate the materials covered by looking for a
12 particular directory or name. However, in other cases, such techniques may not yield the
13 evidence described in the warrant. Individuals may mislabel or hide files and directories;
14 encode communications to avoid using keywords; attempt to delete files to evade
15 detection; or take other steps designed to hide information from law enforcement
16 searches for information.

17 46. The search procedure of any digital device seized may include the
18 following on-site techniques to seize the evidence authorized in Attachment B:
19
20
21
22
23
24
25
26
27
28

1 a. On-site triage of computer systems to determine what, if any,
2 peripheral devices or digital storage units have been connected to such computer systems,
3 a preliminary scan of image files contained on such systems and digital storage devices to
4 help identify any other relevant evidence or co-conspirators.

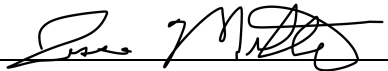
5 b. On-site copying and analysis of volatile memory, which is usually
6 lost if a computer is powered down, and may contain information about how the
7 computer is being used, by whom, when and may contain information about encryption,
8 virtual machines, or steganography which will be lost if the computer is powered down.

9 c. On-site forensic imaging of any computers may be necessary for
10 computers or devices that may be partially or fully encrypted in order to preserve
11 unencrypted data that may, if not immediately imaged on-scene become encrypted and
12 accordingly become unavailable for any examination.

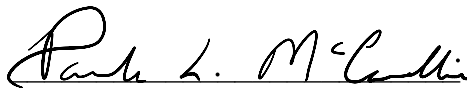
13 47. *Nature of examination.* Based on the foregoing, and consistent with Rule
14 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise
15 copying storage media that reasonably appear to contain some or all of the evidence
16 described in the warrant, and would authorize a later review of the media or information
17 consistent with the warrant. The later review may require techniques, including but not
18 limited to computer-assisted scans of the entire medium, that might expose many parts of
19 a hard drive to human inspection in order to determine whether it is evidence described
20 by the warrant.
21
22
23
24
25
26
27
28

CONCLUSION

48. Based on the information set forth herein, there is probable cause to search the above described SUBJECT PREMISES and SUBJET VEHICLES, as further described in Attachment A, as well as on and in any digital device or other electronic storage media found, for evidence, fruits and instrumentalities, as further described in Attachment B, of the TARGET OFFENSES.


Jesse Miller, Special Agent
Department of Homeland Security
Homeland Security Investigations

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 8th day of March 2021.


PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A**Description of Property to be Searched**

The physical address of the SUBJECT PREMISES is 3407 Woburn Street, Apartment 112, Bellingham, Washington 98226, and is more fully described as an apartment within a multi-unit dwelling. The door of Apartment 112 is black and bears the number "112"

The search is to include all rooms and persons within the SUBJECT PREMISES and all garage/parking spaces, or storage areas assigned to Apartment 112, as well as any digital device(s) found therein.





Description of the SUBJECT VEHICLES

SUBJECT VEHICLE 1 is a 2016 Grand Caravan , bearing Washington License Plate #BHR0403.

SUBJECT VEHICLE 2 is a 2014 Volkswagen Jetta, bearing Washington License Plate #AR14245.

The search of SUBJECT VEHICLES 1 and 2 is to include the entirety of the vehicles, any close containers, and any digital devices found therein.

ATTACHMENT B
ITEMS TO BE SEIZED

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) committed in or after November 2020 as follows:

- a. Items, records, or information³ relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- c. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- d. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- e. Items, records, or information related to communications with or about minors;
- f. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- g. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence,

³ As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

1 purchase or lease agreements, diaries, statements, identification documents,
2 address books, telephone directories, and keys;

3 h. Items, records, or information concerning the ownership or use of computer
4 equipment found in the SUBJECT PREMISES, including, but not limited
5 to, sales receipts, bills for internet access, handwritten notes, and computer
6 manuals;

7 i. Any digital devices or other electronic storage media⁴ and/or their
8 components including:

9 i. any digital device or other electronic storage media capable of being
10 used to commit, further, or store evidence, fruits, or instrumentalities
11 of the offenses listed above;

12 ii. any magnetic, electronic or optical storage device capable of storing
13 data, including thumb drives, SD cards, or external hard drives;

14 iii. any physical keys, encryption devices, dongles and similar physical
15 items that are necessary to gain access to the computer equipment,
16 storage devices or data; and

17 iv. any passwords, password files, test keys, encryption codes or other
18 information necessary to access the computer equipment, storage
19 devices or data.

20 j. For any digital device or other electronic storage media whose seizure is
21 otherwise authorized by this warrant, and any digital device or other
22 electronic storage media that contains or in which is stored records or
23 information that is otherwise called for by this warrant:

24 i. evidence of who used, owned, or controlled the digital device or
25 other electronic storage media at the time the things described in this
26 warrant were created, edited, or deleted, such as logs, registry
27 entries, configuration files, saved usernames and passwords,
28

26 ⁴ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical,
27 or other high speed data processing devices performing logical, arithmetic, or storage functions,
28 including desktop computers, notebook computers, mobile phones, tablets, server computers, and
network hardware. The term “electronic storage media” includes any physical object upon
which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash
memory, CD-ROMs, and other magnetic or optical media.

1 documents, browsing history, user profiles, email, email contacts,
2 “chat,” instant messaging logs, photographs, and correspondence;

3 ii. evidence of software that would allow others to control the digital
4 device or other electronic storage media, such as viruses, Trojan
5 horses, and other forms of malicious software, as well as evidence of
6 the presence or absence of security software designed to detect
7 malicious software;

8 iii. evidence of the lack of such malicious software;

9 iv. evidence of the attachment to the digital device of other storage
10 devices or similar containers for electronic evidence;

11 v. evidence of counter-forensic programs (and associated data) that are
12 designed to eliminate data from the digital device or other electronic
13 storage media;

14 vi. evidence of the times the digital device or other electronic storage
15 media was used;

16 vii. passwords, encryption keys, and other access devices that may be
17 necessary to access the digital device or other electronic storage
18 media;

19 viii. documentation and manuals that may be necessary to access the
20 digital device or other electronic storage media or to conduct a
21 forensic examination of the digital device or other electronic storage
22 media;

23 ix. records of or information about the Internet Protocol used by the
24 digital device or other electronic storage media;

25 x. records of internet activity, including firewall logs, caches, browser
26 history and cookies, “bookmarked” or “favorite” web pages, search
27 terms that the user entered into any internet search engine, and
28 records of user-typed web addresses.

xi. contextual information necessary to understand the evidence
described in this attachment.

1 This warrant authorizes a review of electronic storage media and electronically stored
2 information seized or copied pursuant to this warrant in order to locate evidence, fruits,
3 and instrumentalities described in this warrant. The review of this electronic data may be
4 conducted by any government personnel assisting in the investigation, who may include,
5 in addition to law enforcement officers and agents, attorneys for the government, attorney
6 support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete
7 copy of the seized or copied electronic data to the custody and control of attorneys for the
8 government and their support staff for their independent review.

9 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
10 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
11 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
12 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
13 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
14 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
15 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
16 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
17 CRIMES.
18
19
20
21
22
23
24
25
26
27
28